## LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended)      A method for cross directory authentication in a Public Key Infrastructure (PKI) comprising:

configuring a first directory to query a second directory when receiving queries regarding signature certificates from a second enterprise PKI, the first directory being part of a first enterprise PKI, the second directory being part of the second enterprise PKI;

configuring the first directory with information regarding users with signature certificates associated with the second enterprise PKI that are allowed access to the server;

attempting access to a server by a user, the server being part of the first enterprise PKI, the user presenting a signature certificate from the second enterprise PKI to the server for authentication;

sending a query to the first directory from the server to determine if the user is allowed access to the server;

sending a query to the second directory from the first directory to determine if the user is a member of the second enterprise PKI; and

signaling the server by the first directory that the user is allowed access to the server if the user is a member of the second enterprise PKI.

2. (Original)    The method according to claim 1, further comprising configuring the first directory by a network administrator.

3. (Original)    The method according to claim 1, further comprising configuring the server with information regarding users with signature certificates from the second enterprise PKI that are allowed access to the server.

4. (Canceled)

5. (Currently Amended)      The method according to claim [[4]]1, further comprising configuring the server by a network administrator.

6. (Currently Amended)      A system for cross directory authentication in a Public Key Infrastructure (PKI) comprising:

      at least one server, the at least one server being part of a first enterprise PKI;

      at least one client platform, the at least one client platform usable by at least one user to request access to the at least one server;

      a second directory, the second directory containing information on at least one user with a signature certificate for a second enterprise PKI, the second directory being part of the second enterprise PKI; and

      a first directory, the first directory sending a query to the second directory when receiving a query from at least one server regarding a signature certificate for the second enterprise PKI received at the at least one server from at least one user for authentication, the query from the at least one server sent to the first directory to determine if the at least one user is allowed access to the at least one server, the first directory being part of the first enterprise PKI and including a directory entry that includes users with signature certificates from the second enterprise PKI that are allowed access to the server, the query sent to the second directory from the first directory being sent to determine if the at least one user is a member of the second enterprise PKI, the first directory signaling the at least one server that the at least one user is allowed access to the at least one server if the user is a member of the second enterprise PKI.

7. (Original)   The system according to claim 6, wherein the first directory comprises a database.

8. (Original)   The system according to claim 6, wherein the second directory comprises a database.

9. (Original)   The system according to claim 6, wherein the at least one server, the at least one client platform, and the first directory are operably connected via a network.

10. (Currently Amended)      An article comprising a storage medium having instructions stored therein, the instructions when executed causing a processing device to perform:

receiving configuration information that causes the processing device to send a query to a directory when receiving queries regarding signature certificates for a second enterprise PKI, the processing device being part of a first enterprise PKI, the directory being part of the second enterprise PKI;

receiving a query from a server requesting if a user is allowed access to the server, the server being part of the first enterprise PKI and including a directory entry including users with signature certificates from the second enterprise PKI that are allowed access to the server;

sending a query to the directory to determine if the user is a member of the second enterprise PKI; and

signaling the server that the user is allowed access to the server if the user is a member of the second enterprise PKI.